

Art Unit: ***

March 30, 2005

CLMPTO

AS

1. A digital data protection arrangement comprising executable code which incorporates sufficient information relating to the protected data to be able to create, when executed, further code which contains the protected data in usable form.
2. The arrangement of claim 1, comprising security means operable to detect corruption of the protected data, the further code incorporating at least one instruction to call the security means to assess any corruption.
3. The arrangement of claim 2, wherein the call instruction is contained within the further code at the required location of a set of executable code, and wherein the security means is operable to recreate the set of executable code when executed, to replace the call instruction.
4. The arrangement of claim 2, wherein the security means is operable to delete the further code in the event that any corruption is detected.
5. The arrangement of claim 2, wherein the security means is operable to decrypt encrypted code located at the required location, and to replace the encrypted code with corresponding decrypted code.
6. The arrangement of claim 2, wherein the security means is embedded within the further code.
7. The arrangement of claim 6, wherein the security means is embedded at locations which are unused by the further code.
8. The arrangement of claim 7, wherein at least one embedding location is identified when the executable code is executed, the security means is written to the embedding location.

Art Unit: ***

9. The arrangement of claim 8, wherein an embedding location is identified by decompiling the further code, and analysing the decompiled code.

10. The arrangement of claim 2, the arrangement further comprising relocation means operable to change the location of the security means and to modify the call instruction to refer to the new location.

11. The arrangement of claim 10, wherein the relocation means is contained within the protected data, to operate repeatedly while the protected code is in use.

12. The arrangement of claim 1, wherein the executable code contains executable instructions for creating the protected code.

13. The arrangement of claim 1, wherein the executable code incorporates the protected data in encrypted form, together with executable instructions for decryption.

14. The arrangement of claim 13, wherein initial execution of the executable code installs the decryption instructions for execution, subsequent execution of the decryptic instructions causing decryption of the protected data.

15. The arrangement of claim 14, wherein the decryption instructions are initially stored in non-executable form and require execution to authorise execution of the protected software, the arrangement further including conversion means operable to convert the said block of code to an executable form by means of an algorithm which requires at least one conversion key, and further operable to derive a conversion key, for use in the algorithm, by reference to a target block of code which is in executable or non-executable form, whereby an appropriate conversion key will be derived only if the target block is unmodified.

16. The arrangement of claim 15, wherein the security means comprises a

Art Unit: ***

plurality of blocks of executable code stored in non-executable form and each of which requires execution to authorise execution of the protected software, the conversion means being operable to convert each block to executable form.

17. The arrangement of claim 16, wherein conversion of each block is achieved by a conversion key derived from a respective target block.

18. The arrangement of claim 16, wherein at least one block is operable, upon execution, to convert another block to an executable form for subsequent execution.

19. The arrangement of claim 18, wherein each block is operable, upon execution, to convert another block to an executable form for subsequent execution.

20. The arrangement of claim 15, wherein the or each target block is contained within the protected software.

21. The arrangement of claim 15, wherein the or each target block is contained within the first security means.

22. The arrangement of claim 15, wherein the or each algorithm for converting code include a CRC algorithm.

23. The arrangement of claim 1, wherein the protected data contains executable code and/or a data file.

24. The arrangement of claim 1, comprising processing means operable to execute code, and memory means within which the said executable code is stored, the executable code being stored in the memory means with a start point at a memory location indicated within the arrangement as the start point for the protected data, whereby the processor means will cause the said executable code to be executed when seeking to access the protected data.

Art Unit: ***

25. The arrangement of claim 1, wherein the executable code is operable to recreate the protected data in substantially unencrypted form.

26. The arrangement of claim 1, wherein the protected data contains at least one executable instruction which contains a plurality of steps, the steps being executable in more than one order to implement the instruction, and the executable code being operable to create the instruction by creating the steps in an order which changes on each execution of the executable code.

27. The arrangement of claim 26, wherein the order of the steps is chosen substantially at random on each execution.

28. The arrangement of claim 26, wherein the steps include at least one step which initiates the operation of security means operable to detect corruption of the protected data.

29. The arrangement of claim 26, wherein the executable code is executable to create the steps on each occasion that the executable instruction is to be executed.

30. The arrangement of claim 1, wherein the executable code is arranged to provide, upon each execution, a part of the protected data in usable form and other data in corrupt form, whereby more than one execution is required to provide the whole of the protected data in usable form.

31. The arrangement of claim 30, wherein each part corresponds with a complete executable routine within the protected data, whereby a complete set of routines forming the protected data can be created by repeated execution of the executable code.

32. The arrangement of claim 30, wherein each execution of the executable code causes previously created usable code to be corrupted, whereby only the code created by the most recent execution will be in usable form during

Art Unit: ***

25. The arrangement of claim 1, wherein the executable code is operable to recreate the protected data in substantially unencrypted form.

26. The arrangement of claim 1, wherein the protected data contains at least one executable instruction which contains a plurality of steps, the steps being executable in more than one order to implement the instruction, and the executable code being operable to create the instruction by creating the steps in an order which changes on each execution of the executable code.

27. The arrangement of claim 26, wherein the order of the steps is chosen substantially at random on each execution.

28. The arrangement of claim 26, wherein the steps include at least one step which initiates the operation of security means operable to detect corruption of the protected data.

29. The arrangement of claim 26, wherein the executable code is executable to create the steps on each occasion that the executable instruction is to be executed.

30. The arrangement of claim 1, wherein the executable code is arranged to provide, upon each execution, a part of the protected data in usable form and other data in corrupt form, whereby more than one execution is required to provide the whole of the protected data in usable form.

31. The arrangement of claim 30, wherein each part corresponds with a complete executable routine within the protected data, whereby a complete set of routines forming the protected data can be created by repeated execution of the executable code.

32. The arrangement of claim 30, wherein each execution of the executable code causes previously created usable code to be corrupted, whereby only the code created by the most recent execution will be in usable form during

Claim 33 (canceled)

Art Unit: ***

34. A data carrier containing software which, when installed on a computer system, is operable as a digital data protection arrangement in accordance with claim 1.

35. Computer software which, when installed on a computer system, is operable as a digital data protection arrangement in accordance with claim 1.

36. Computer software operable to provide protection for a second item of computer software, the protection software comprising security means operable to authorise execution of the protected software in response to successful completion of one or more security checks, and having at least one block of executable code which is stored in non-executable form and which requires execution to authorise execution of the protected software, and the protection software further comprising conversion means operable to convert the said block of code to an executable form by means of an algorithm which requires at least one conversion key, the conversion means being further operable to derive a conversion key, for use in the algorithm, by reference to a target block of code in executable or non-executable form, whereby an appropriate conversion key will be derived only if the target block is unmodified.

37. A computer memory device containing computer software in accordance with claim 36.

38. A computer system containing an item of computer software protected by means of computer software in accordance with claim 36.

39. (New) A computer system comprising memory means containing a digital protection arrangement according to claim 1.